OCRS 2023

Manufacturing Cyber Resilience

PEAK | IT
SECURITY & SOLUTIONS

Nancy Laney, CyberAB Registered Practitioner

Owner PEAK Complyance CyberAB Registered Practitioner Organization

Nancy Laney is President and Owner of PEAK Complyance, a division of Laney ITC (RPO) in Southern Oregon, focusing on bringing the expertise of over 30 years of compliance design and implementation within reach of the SMB in the defense industrial base. She is a CMMC Registered Professional and has professional certifications in Project Management (PMP), Healthcare Information and Management Systems (CPHIMS), and has implemented many certification standards including ITIL, HIPAA, CIS and NIST.

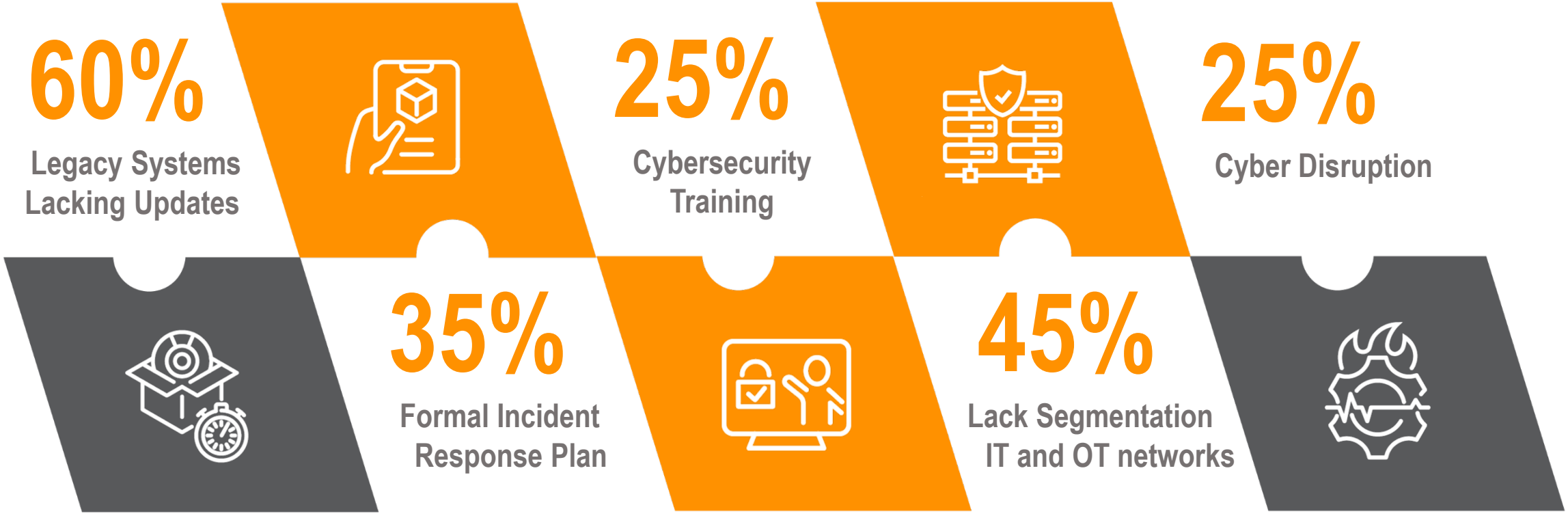
Nancy's mission is to make the complex understandable; to distill the possibilities of best practices to exactly what is needed for small business.

Prior to launching both her MSP (PEAK IT Security & Services) and PEAK Complyance, Nancy served as an IT consultant, Corporate IT Director, Program Manager, as well as New Construction IT Project Manager in healthcare related fields for national healthcare companies.

https://www.linkedin.com/in/nancylaney/

PEAK | IT
SECURITY & SOLUTIONS

Current State of Manufacturing



www.cobalt.io/blog/cybersecurity-statistics-2023

Threats to IT & OT Manufacturing

60%
SMB Owners Think they are NOT a Target

38%
Server Security Misconfigurations

96%
Focused on Monetary Gain

14%
Prepared to Defend Cyberattack

95%
Data Breaches Due To Human Error

www.cobalt.io/blog/cybersecurity-statistics-2023

Hardware / Software

Inventory & Lifecycle

Technology Debt

Inventory

Prioritize

Strategies

Leverage

Documentation

Maintenance & Patching

Servers

Endpoints

Automation

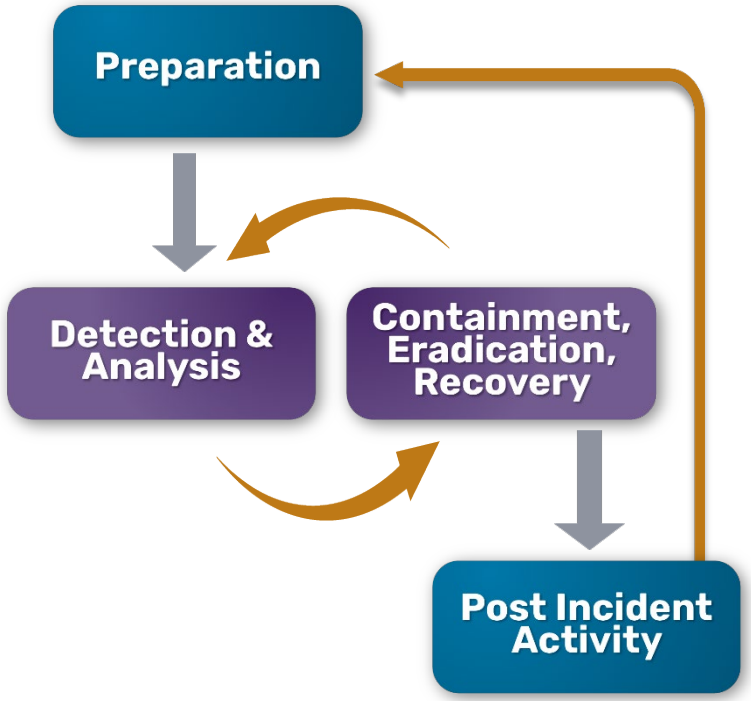
Relentless

“Legacy devices were often deployed on flat networks, at a time when the need for security took a back seat to other priorities, such as high availability and performance.”

Incident Response & Business Continuity

Incident Response Plan

Business Continuity Disaster Recovery



3-2-1-1-0

Immutable Backups

Air gapped

Critical

Business Priorities

Downtime

Network

DMZ & Firewall

- Public Facing
- Ports
- Configuration
- Documentation

Segmentation

- Unmanged Hubs
- VLANs
- Access Contol Lists
- 802.1x
- DHCP/IPs
- Layers of security
- Documentation

Endpoints

Configuration Management

- Patch/update
- Domain Joined
- Manage Stale AD
- Full Disk Encryption
- LAPS
- No Personal SW

Anti-Virus

- Endpoints
- Servers
- AV Current
- Behavior Based
- Zero-Trust

Users

Training

Human Shield

Train Often

Phishing Campaigns

Cheat Sheets

Password Strength

Password Manager

Least Privilege

Least Privilege

Role Based Access

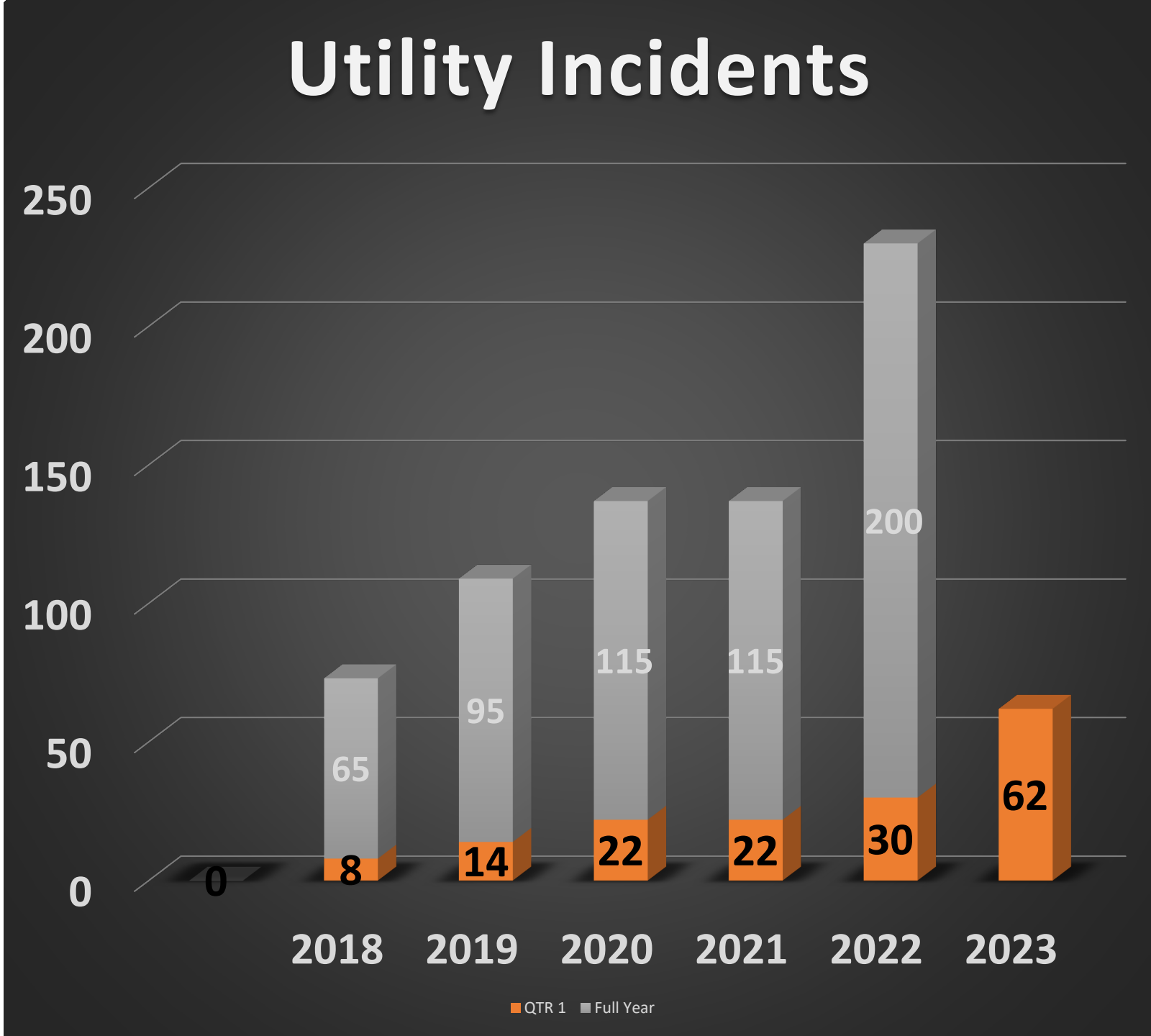
MFA

2FA

MFA

TOTP

Threats to IT & OT Critical Infrastructure



According to Politico 9/10/2023:
https://www.politico.com/news/2023/09/10/power-grid-attacks

1 Day Away

1. Immutable Backup & Test it
2. Relentless Patching
3. Upgrade to current versions
4. Anti-Virus
5. 2FA on EVERYTHING
6. Strong Passwords
    a) Password Manager
7. Network Segmentation
8. Incident Response Plan
9. PingCastle/Testimo
10. ATP Recommendations

PEAK IT
SECURITY & SOLUTIONS

Nancy@peakitss.com

3.5 Million

of Open Cybersecurity Jobs in 2023 waiting to be filled

Thank you!

PEAK | IT
SECURITY & SOLUTIONS